

**Family list**

**1** family member for:

**JP2002269043**

Derived from 1 application.

- 1**    **INFORMATION PROCESSOR, INFORMATION PROCESSING SYSTEM,  
USER AUTHENTICATION PROCESSING METHOD AND STORAGE  
MEDIUM**

Publication info: **JP2002269043 A** - 2002-09-20

---

Data supplied from the **esp@cenet** database - Worldwide

000000 PAGE BLANK (USPTO)

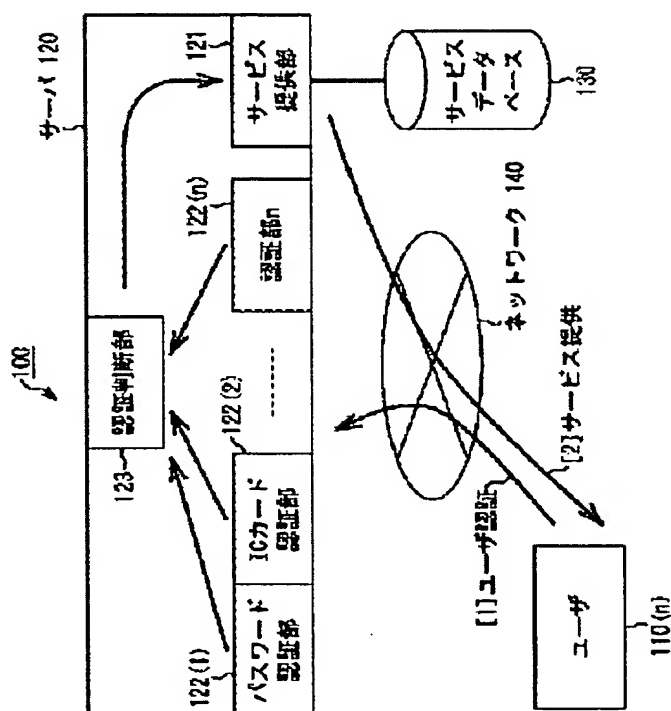
**INFORMATION PROCESSOR, INFORMATION PROCESSING SYSTEM, USER AUTHENTICATION PROCESSING METHOD AND STORAGE MEDIUM**

**Patent number:** JP2002269043  
**Publication date:** 2002-09-20  
**Inventor:** TAGASHIRA NOBUHIRO; SUGA YUJI; WAKAO SATOSHI  
**Applicant:** CANON KK  
**Classification:**  
- international: G06F15/00; H04L9/32  
- european:  
**Application number:** JP20010067211 20010309  
**Priority number(s):** JP20010067211 20010309

Report a data error here

**Abstract of JP2002269043**

**PROBLEM TO BE SOLVED:** To provide an information processing system corresponding to various service supply forms. **SOLUTION:** In an information processor 120 authenticating a user based on information by a request from a user 110(n), user authentication means 122 (1), 122(2),..., and 122(n) authenticate the user by an arbitrary user authentication method. An authentication judging means 123 finally decides a stepwise user authentication result with respect to the user based on the authentication results in the user authentication means 122(1), 122(2),..., and 122(n).



Data supplied from the esp@cenet database - Worldwide

PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-269043  
(P2002-269043A)

(43) 公開日 平成14年9月20日 (2002.9.20)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	マークシート (参考)
G 0 6 F 15/00	3 3 0	C 0 6 F 15/00	3 3 0 D 5 B 0 8 6
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A 5 J 1 0 4
			6 7 3 D
			6 7 3 E
			6 7 5 D
審査請求 未請求 請求項の数15 O L (全 17 頁)			

(21) 出願番号 特願2001-67211(P2001-67211)

(22) 出願日 平成13年3月9日 (2001.3.9)

(71) 出願人 000001007

キヤノン株式会社  
東京都大田区下丸子3丁目30番2号

(72) 発明者 田頭 信博

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(72) 発明者 須賀 祐治

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74) 代理人 100090273

弁理士 國分 孝悦

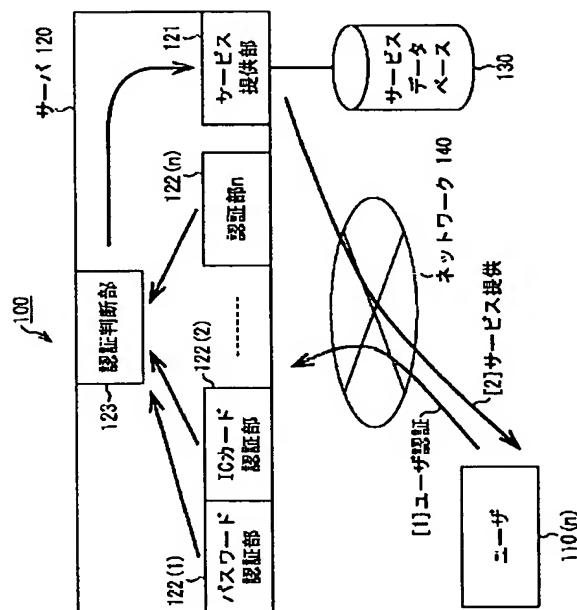
最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理システム、ユーザ認証処理方法、及び記憶媒体

(57) 【要約】

【課題】 多様なサービス提供形態に対応できる情報処理システムを提供する。

【解決手段】 ユーザ110(n)からの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置120において、ユーザ認証手段122(1)、1220(2)、…、122(n)は、任意のユーザ認証方法によりユーザ認証を行う。認証判断手段123は、ユーザ認証手段122(1)、1220(2)、…、122(n)での認証結果に基づいて、ユーザに対する段階的なユーザ認証結果を最終決定する。



【特許請求の範囲】

【請求項1】 ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、任意のユーザ認証方法により上記ユーザ認証を行う少なくとも1つのユーザ認証手段と、上記ユーザ認証手段での認証結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする情報処理装置。

【請求項2】 上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせに基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする請求項1記載の情報処理装置。

【請求項3】 ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、任意のユーザ認証方法により上記ユーザ認証を行う少なくとも1つのユーザ認証手段と、上記ユーザの存在位置を検出する検出手段と、上記ユーザ認証手段での認証結果及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする情報処理装置。

【請求項4】 上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせ、及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする請求項3記載の情報処理装置。

【請求項5】 上記ユーザ認証方法は、パスワードを用いた認証方法、情報記録された記憶媒体を用いた認証方法、及びバイオメトリクスを用いた認証方法の少なくとも何れかの方法を含むことを特徴とする請求項1又は3記載の情報処理装置。

【請求項6】 上記認証判断手段で決定されたユーザ認証結果に基づいて、上記ユーザに対して任意のサービスを提供するサービス提供手段を備えることを特徴とする請求項1又は3記載の情報処理装置。

【請求項7】 上記サービス提供手段は、段階的な上記サービスを提供することを特徴とする請求項6記載の情報処理装置。

【請求項8】 複数の機器が互いに通信可能に接続される情報処理システムであって、上記複数の機器のうち少なくとも1つの機器は、請求項1～7の何れかに記載の情報処理装置の機能を有することを特徴とする情報処理システム。

【請求項9】 ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせに基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とする

ユーザ認証処理方法。

【請求項10】 ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、上記ユーザからの要求がなされた装置或いはシステムの位置情報を検出する位置検出ステップと、上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせ、及び上記位置検出ステップによる検出結果に基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とするユーザ認証処理方法。

【請求項11】 上記単一又は複数のユーザ認証ステップは、パスワードを用いたユーザ認証を行うステップ、情報記録された記憶媒体を用いたユーザ認証を行うステップ、及びバイオメトリクスを用いたユーザ認証を行うステップの少なくとも何れかのステップを含むことを特徴とする請求項9又は10記載のユーザ認証処理方法。

【請求項12】 上記認証判断ステップにより最終決定されたユーザ認証結果に基づいて、上記ユーザ側に対して任意のサービスを提供するサービス提供ステップを含むことを特徴とする請求項9又は10記載のユーザ認証処理方法。

【請求項13】 上記サービス提供ステップは、段階的な上記サービスを提供するステップを含むことを特徴とする請求項12記載のユーザ認証処理方法。

【請求項14】 請求項1～7の何れかに記載の情報処理装置の機能、又は請求項8記載の情報処理システムの機能をコンピュータに実現させるためのプログラムを記録したコンピュータ読出可能な記憶媒体。

【請求項15】 請求項9～13の何れかに記載のユーザ認証処理方法の処理ステップをコンピュータに実行させるためのプログラムを記録したコンピュータ読取可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、ネットワークを介したサービス享受のためのユーザ認証を行う装置或いはシステムに用いられる、情報処理装置、情報処理システム、ユーザ認証処理方法、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体に関するものである。

【0002】

【従来の技術】近年において、インターネットに代表されるネットワークインフラの普及に伴い、ネットワークを利用したサービスが多く提供されるようになった。これらのサービスの中では、“anonymous ftp”に代表されるような、ユーザ認証（ユーザ名とパスワード等を用いた認証）を伴わないサービスが存在するが、“Telnet (telecommunication)

on network)”及び“rlogin(remote login)”等のような、ユーザ認証を伴うサービスが多く存在する。このような背景のもと、ユーザ認証の方法としては、パスワードやＩＣカード、或いはバイオメトリクス等を用いた様々な方法が提案され実現されている。

【0003】具体的には例えば、ユーザ認証の方法としては、銀行のＣＤやＡＴＭの利用時のパスワード入力による方法、或いは“Telnet”や“rlogin”等のサービスを受ける際のパスワード入力による方法がある。また、建物への入退出管理や計算機利用の管理等を行なうためのＩＣカードによるユーザ認証方法や、高度な機密保持が必要な建物への入退出管理を行うための指紋や網膜等によるユーザ認証（バイオメトリクス技術を用いたユーザ認証）方法がある。

【0004】また、近年のＬＡＮ網や、固定電話回線網、或いは無線電話回線網等のネットワークインフラの多様化によって、ユーザがサービスを楽しむための端末装置の多様化も進んでいる。

【0005】上記の端末装置としては、例えば、パーソナルコンピュータ（以下、単に「パソコン」又は「ＰＣ」と言う）が多く利用されている。一般にパソコンはユーザの自宅で利用されるが、近年では、パソコンを店内に設けた所謂インターネットカフェが多く利用されている。これにより、ユーザは、自宅のＰＣでサービスを楽しむことが可能であると共に、インターネットカフェのＰＣでサービスを楽しむことも可能である。

【0006】さらに、上記の端末装置としては、ネットワークを介した通信が可能な携帯電話等の携帯端末装置が利用されており、この携帯端末装置を利用したサービス享受や、上述したＰＣ等を利用したサービス享受等、様々なサービス利用形態が存在している。

【0007】

【発明が解決しようとする課題】しかしながら、上述したような従来のユーザ認証方法は、ユーザに提供するサービスに対して固定の方法のみしか存在しない。例えば、“Telnet”や“rlogin”によるサービス享受のためのユーザ認証は、簡便なパスワードによる方法が用いられている。また、高度に機密保持が必要な建物への入退出管理のためのユーザ認証は、高度なユーザ認証技術であるバイオメトリクスによる方法が用いられている。

【0008】すなわち、従来のユーザ認証方法は、簡便な認証であるか、或いは厳密な認証であるかの差はあるが、何れの認証においても、その認証結果は、「可」又は「不可」の二通りしかない。このため、ユーザ認証結果に応じて、例えば、「サービスを提供する」又は「サービスを提供しない」の二通りの判断しか行えない。したがって、以下に説明するような問題が生じてくる。

【0009】例えば、今後は、ユーザが使用する端末装

置の多様化により、段階的なサービスの提供が考えられる。具体的には、画像を閲覧するサービスに関して、高解像度の画像を表示可能な自宅のＰＣにおいてサービスを楽しむ場合と、低解像度の画像（場合によっては二値画像）しか表示できない携帯端末装置からサービスを楽しむ場合とでは、同じサービスであっても、そのサービスの品質にレベル差がある。また、機密文書を閲覧するサービスに関して、社内から社内の機密文書にアクセスする等の地理的に安全な場所に位置する端末装置からサービスを楽しむ場合と、社外から社内の機密文書にアクセスする等の地理的に安全でない場所に位置する端末装置からサービスを楽しむ場合とでは、同じサービスであっても、そのサービスの機密度合いにレベル差がある。

【0010】しかしながら、上述したように、従来のユーザ認証方法は、提供するサービスに固有のものであり、その認証結果が「可」又は「不可」の二通りしかない、すなわち「サービスを提供する」又は「サービスを提供しない」の二通りの判断しか行えないため、上記のような段階的なサービス提供等の様々なサービス提供形態に適応的に対応できない。

【0011】そこで、本発明は、上記の欠点を除去するために成されたもので、以下の（１）～（３）を実現可能な、情報処理装置、情報処理システム、ユーザ認証処理方法、及びそれを実施するための処理ステップをコンピュータが読出可能に格納した記憶媒体を提供することを目的とする。

（１）多様なサービス提供形態に対応できる。

（２）段階的であって多様なサービスを提供する際に、それぞれのサービスに対応可能である。

（３）ユーザ認証結果に応じて適応的に異なるサービスを提供できる。

【0012】

【課題を解決するための手段】斯かる目的下において、第１の発明は、ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、任意のユーザ認証方法により上記ユーザ認証を行う少なくとも１つのユーザ認証手段と、上記ユーザ認証手段での認証結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする。

【0013】第２の発明は、上記第１の発明において、上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせに基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする。

【0014】第３の発明は、ユーザからの要求による情報に基づいて、当該ユーザ認証を行う情報処理装置であって、任意のユーザ認証方法により上記ユーザ認証を行う少なくとも１つのユーザ認証手段と、上記ユーザの存

在位置を検出する検出手段と、上記ユーザ認証手段での認証結果及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定する認証判断手段とを備えることを特徴とする。

【0015】第4の発明は、上記第3の発明において、上記認証判断手段は、複数の上記ユーザ認証手段での複数の認証結果の組み合わせ、及び上記検出手段での検出結果に基づいて、上記ユーザに対する段階的なユーザ認証結果を決定することを特徴とする。

【0016】第5の発明は、上記第1又は3の発明において、上記ユーザ認証方法は、パスワードを用いた認証方法、情報記録された記憶媒体を用いた認証方法、及びバイオメトリクスを用いた認証方法の少なくとも何れかの方法を含むことを特徴とする。

【0017】第6の発明は、上記第1又は3の発明において、上記認証判断手段で決定されたユーザ認証結果に基づいて、上記ユーザに対して任意のサービスを提供するサービス提供手段を備えることを特徴とする。

【0018】第7の発明は、上記第6の発明において、上記サービス提供手段は、段階的な上記サービスを提供することを特徴とする。

【0019】第8の発明は、複数の機器が互いに通信可能に接続されてなる情報処理システムであって、上記複数の機器のうち少なくとも1つの機器は、請求項1〜7の何れかに記載の情報処理装置の機能を有することを特徴とする。

【0020】第9の発明は、ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせに基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とする。

【0021】第10の発明は、ユーザからの要求に基づいて、当該ユーザ認証を行うためのユーザ認証処理方法であって、上記ユーザに対してユーザ認証を行う単一又は複数のユーザ認証ステップと、上記ユーザからの要求がなされた装置或いはシステムの位置情報を検出する位置検出ステップと、上記単一又は複数のユーザ認証ステップによる認証結果の組み合わせ、及び上記位置検出ステップによる検出結果に基づいて、段階的なユーザ認証結果を最終決定する認証判断ステップとを含むことを特徴とする。

【0022】第11の発明は、上記第9又は10の発明において、上記単一又は複数のユーザ認証ステップは、パスワードを用いたユーザ認証を行うステップ、情報記録された記憶媒体を用いたユーザ認証を行うステップ、及びバイオメトリクスを用いたユーザ認証を行うステップの少なくとも何れかのステップを含むことを特徴とする。

【0023】第12の発明は、上記第9又は10の発明において、上記認証判断ステップにより最終決定されたユーザ認証結果に基づいて、上記ユーザ側に対して任意のサービスを提供するサービス提供ステップを含むことを特徴とする。

【0024】第13の発明は、上記第12の発明において、上記サービス提供ステップは、段階的な上記サービスを提供するステップを含むことを特徴とする。

【0025】第14の発明は、請求項1〜7の何れかに記載の情報処理装置の機能、又は請求項8記載の情報処理システムの機能をコンピュータに実現させるためのプログラムをコンピュータ読出可能な記憶媒体に記録したことを特徴とする。

【0026】第15の発明は、請求項9〜13の何れかに記載のユーザ認証処理方法の処理ステップをコンピュータに実行させるためのプログラムをコンピュータ読出可能な記憶媒体に記録したことを特徴とする。

【0027】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【0028】[第1の実施の形態]本発明は、例えば、図1に示すようなネットワークシステム100に適用される。

【0029】まず、本実施の形態のネットワークシステム100の具体的な説明の前に、本実施の形態での基本とする目的は、多様なサービスを提供するために多様なユーザ認証結果を得ることである。本実施の形態における“多様なユーザ認証結果”とは、従来のようなユーザ認証結果としての「可」又は「不可」の二値の結果ではなく、多値の結果を意味する。

【0030】多値のユーザ認証結果を得るための構成としては様々なものが考えられる。例えば、パスワードを用いたユーザ認証では、入力されたパスワードの文字数に対する合致した文字数の割合に基づいて、ユーザ認証結果を多値で出力する。また、指紋を用いたユーザ認証では、指紋画像の類似度合いに基づいて、ユーザ認証結果を多値で出力する。

【0031】しかしながら、あるユーザ認証方法においてユーザ認証結果を多値化した場合でも、最終的なユーザ認証結果の決定に作用する情報は1種類のみである。例えば、パスワードを用いたユーザ認証では、当該パスワードの文字列情報のみが、ユーザ認証結果の決定に作用する。また、指紋を用いたユーザ認証では、指紋画像のみのみが、ユーザ認証結果の決定に作用する。

【0032】すなわち、多様なサービスを提供するための多様なユーザ認証結果を得る構成としては、ユーザ認証方法に依存した1種類の情報からの多値のユーザ認証結果だけでは、十分な多様性を持つことができないと考えられる。

【0033】そこで、本実施の形態のネットワークシス



テム100では、以下に説明するような構成により、独立した複数のユーザ認証方法（以下、「ユーザ認証方式」とも言う）により多様なユーザ認証結果を得ることを実現している。

【0034】＜ネットワークシステム100の全体構成＞ネットワークシステム100は、上記図1に示すように、ユーザ側の端末装置110(n)と、サービスデータベース130を有するサーバ120(m)とが、ネットワーク140を介して互いに通信可能なように接続された構成としている。

【0035】尚、上記図1では、説明の簡単のため、ネットワーク140に接続されているユーザ側の端末装置として、1つのユーザ側の端末装置110(n)のみ図示しているが、この接続数に限られることはない。本実施の形態では、例えば、複数のユーザ側の端末装置がネットワーク140に接続されており、これらの複数のユーザ側の端末装置の中の任意の端末装置110(n)に着目している。また、サーバ120についても同様に、ネットワーク140に接続されているサーバとして、1つのサーバ120のみ図示しているが、この接続数に限られることはない。

【0036】ユーザ側の端末装置110(n)、及びサーバ120は、例えば、図2に示すようなコンピュータ機能200により、後述するような各種機能を実現するようになされている。

【0037】コンピュータ機能200は、上記図2に示すように、CPU201と、ROM202と、RAM203と、キーボード(KB)209のキーボードコントローラ(KBC)205と、表示部としてのCRTディスプレイ(CRT)210のCRTコントローラ(CRTC)206と、ハードディスク(HD)211及びフロッピー（登録商標）ディスク(FD)212のディスクコントローラ(DKC)207と、ネットワーク140に接続されたネットワークインターフェースカード(NIC)208とが、システムバス204を介して互いに通信可能に接続された構成としている。

【0038】CPU201は、ROM202或いはHD211に記憶されたソフトウェア、或いはFD212より供給されるソフトウェアを実行することで、システムバス204に接続された各構成部を総括的に制御する。すなわち、CPU201は、所定の処理シーケンスに従った処理プログラムを、ROM202、或いはHD211、或いはFD212から読み出して実行することで、後述する本実施の形態での動作を実現するための制御を行う。

【0039】RAM203は、CPU201の主メモリ或いはワークエリア等として機能する。KBC205は、KB209や図示していないポインティングデバイス等からの指示入力を制御する。CRTC206は、CRT210の表示を制御する。DKC207は、ブート

プログラム、種々のアプリケーション、編集ファイル、ユーザファイル、ネットワーク管理プログラム、及び本実施の形態を実現するための所定の処理プログラム等を記憶するHD211及びFD212とのアクセスを制御する。NIC208は、ネットワーク140上の装置或いはシステムと双方向にデータをやりとりする。

【0040】ユーザ側の端末装置110(n)は、上記図2のコンピュータ機能200を有するパーソナルコンピュータ等を含み、ユーザからの操作に従って、ネットワーク140を介してサーバ120へアクセス等する。

【0041】サーバ120は、詳細は後述するが、ユーザ側の端末装置110(n)からのアクセスに基づいて、任意のサービスを提供する機能を有し、本実施の形態の最も特徴とする構成である。

【0042】＜サーバ120の構成＞ネットワークシステム100の特徴とする構成はサーバ120にあり、このサーバ120は、特に、提供するサービスに関する情報を記憶したデータベース130と連動して動作するサービス提供部121と、複数のユーザ認証部122

(1), 122(2), ..., 122(n)と、複数のユーザ認証部122(1), 122(2), ..., 122(n)のユーザ認証結果に基づいて最終的なユーザ認証結果を判断する認証判断部123とを含み、これらの構成部121、122(1), 122(2), ..., 122(n)、及び123等により、ユーザ側の端末装置110(n)からのサービス要求を受け付け、当該要求に含まれるユーザ認証に必要な情報を用いたユーザ認証の結果に従って、当該要求により示されるサービスを、ユーザ側の端末装置110(n)に提供する。

【0043】複数のユーザ認証部122(1), 122(2), ..., 122(n)は、入力パスワードによりユーザ認証を行うユーザ認証部122(1)(パスワード認証部)や、ICカードに記憶された情報によりユーザ認証を行うユーザ認証部122(2)(ICカード認証部)等を含んでいる。これらの複数のユーザ認証部122(1), 122(2), ..., 122(n)に対して、単一の認証判断部123が設けられている。

【0044】例えば、ユーザ認証部122(1)は、ユーザ側の端末装置110(n)からの、パスワード入力によるサービス要求(サービスを受けるためのユーザ認証の要求を含む)を受け付る。認証判断部123は、上記の入力パスワードと、サービスデータベース130内に予め秘密に保管している、該当サービスを受ける権利のあるユーザのパスワードとを比較し、これらのパスワードが一致した場合に、正しくユーザ認証されたと判断する。

【0045】また、ユーザ認証部122(2)は、ユーザ側の端末装置110(n)からの、ICカード入力によるサービス要求(サービスを受けるためのユーザ認証の要求を含む)を受け付る。認証判断部123は、上記の

ＩＣカード上の情報と、サービスデータベース１３０内に予め秘密に保管している、該当サービスを受ける権利のあるユーザのＩＣカード上の情報とを比較し、これらのカード情報が一致した場合に、正しくユーザ認証されたと判断する。

【００４６】尚、複数のユーザ認証部１２２（１）、１２２（２）、・・・、１２２（ｎ）としては、上述したパスワードによりユーザ認証するユーザ認証部１２２（１）や、ＩＣカードによりユーザ認証するユーザ認証部１２２（２）に限られることなく、指紋や声紋、或いは網膜パターン等の生体情報を利用したユーザ認証方法等のような、任意のユーザ認証方法でユーザ認証を行うユーザ認証部を含めるようにしてもよい。

【００４７】認証判断部１２３は、詳細は後述するが、上述のような複数のユーザ認証部１２２（１）、１２２（２）、・・・、１２２（ｎ）による複数のユーザ認証結果に基づいて、最終的なユーザ認証判断結果を決定する。

【００４８】サービス提供部１２１は、認証判断部１２３の最終的なユーザ認証結果に基づいて、サービス要求のあったユーザ側の端末装置１１０（ｎ）に対して該当するサービスを提供する。

【００４９】尚、サービス提供部１２１が提供するサービスについて、その数及び種類は限られるものではなく、単一或いは複数のサービスを提供可能である。

【００５０】また、ここでの「サービス」とは、「ユーザに対して、あるコンテンツを動作させる」と定義する。例えば、「コンテンツ」が「画像コンテンツ」であって、「動作」が「表示する」と決定した後に、「画像コンテンツを表示する」というサービスの提供が可能となる。

【００５１】また、本実施の形態におけるサービスとしては、様々なサービスを適用可能である。例えば、音声、或いは画像、或いは音楽及び画像等のコンテンツをユーザ側の端末装置１１０（ｎ）へ提供するサービスや、当該コンテンツをユーザ側の端末装置１１０（ｎ）で再生するサービス、或いは当該コンテンツ（画像のコンテンツ等）をユーザ側の端末装置１１０（ｎ）で表示或いは印刷出力するサービス等、様々なサービスを適用可能である。

【００５２】また、上記のサービスについて、例えば、ユーザ側の端末装置１１０（ｎ）へ提供するコンテンツの品質を変化させるようにしてもよい。例えば、ユーザ側の端末装置１１０（ｎ）で再生可能な音声のコンテンツの音質を変化させる。或いは、ユーザ側の端末装置１１０（ｎ）で印刷出力可能な画像のコンテンツの画質を変化させる。これにより、ユーザ側の端末装置１１０（ｎ）に提供するサービスにレベルを持たせることが可能となる。

【００５３】また、ユーザ側の端末装置１１０（ｎ）に

提供するサービスに関する情報は、上述したように、サービスデータベース１３０で保管されているが、これは、サービスデータベース１３０が、コンテンツと動作の双方を保管していることを意味する。

【００５４】＜サーバ１２０の認証判断部１２３の構成＞認証判断部１２３は、複数のユーザ認証部１２２（１）、１２２（２）、・・・、１２２（ｎ）による複数のユーザ認証結果に基づいて、最終的なユーザ認証判断結果を決定する手段である。ここでは説明の簡単のため、ユーザ認証部１２２（１）は、パスワードを用いたユーザ認証を行い、ユーザ認証部１２２（２）は、ＩＣカードを用いたユーザ認証を行い、ユーザ認証部１２２（３）は、指紋画像を用いたユーザ認証を行うものとし、これらの３つのユーザ認証部１２２（１）～１２２（３）による３つのユーザ認証結果に基づいて、認証判断部１２３は、最終的なユーザ認証判断結果を決定するものとする。

【００５５】図３は、上記の場合の、認証判断部１２３におけるユーザ認証判断結果の決定状態の遷移を示したものである。上記図３において、〔０〕～〔７〕で示す各頂点（黒丸点）は、ユーザ認証判断結果の決定後の状態を表し、各頂点を結ぶ各枝は、ユーザ認証された場合の動作を表す。

【００５６】すなわち、頂点〔０〕（“なし”）は、全てのユーザ認証に失敗している状態を表す。頂点〔１〕（“パスワード”）は、パスワードのみユーザ認証されている状態を表す。頂点〔２〕（“ＩＣカード”）は、ＩＣカードのみユーザ認証されている状態を表す。頂点〔３〕（“指紋（指紋画像）”）は、指紋のみユーザ認証されている状態を表す。頂点〔４〕（“パスワード＆ＩＣカード”）は、パスワード及びＩＣカードがユーザ認証されている状態を表す。頂点〔５〕（“パスワード＆指紋”）は、パスワード及び指紋がユーザ認証されている状態を表す。頂点〔６〕（“ＩＣカード＆指紋”）は、ＩＣカード及び指紋がユーザ認証されている状態を表す。頂点〔７〕（“パスワード＆ＩＣカード＆指紋”）は、パスワード、ＩＣカード、及び指紋の全てがユーザ認証されている状態を表す。

【００５７】認証判断部１２３は、上記図３で示される遷移状態に従って、３つのユーザ認証部１２２（１）～１２２（３）による３つのユーザ認証結果（パスワード、ＩＣカード、及び指紋によるユーザ認証結果）に基づいて、最終的なユーザ認証判断結果を段階的に決定する。

【００５８】例えば、認証判断部１２３は、まず、頂点〔０〕（“なし”）の状態を初期状態とする。この初期状態において、パスワードによるユーザ認証に成功した場合（ユーザ認証部１２２（１）のユーザ認証結果がＯＫの場合）、認証判断部１２３は、頂点〔１〕（“パスワード”）の状態へ移行する。次に、この状態において、

ICカードによるユーザ認証に成功した場合（ユーザ認証部122(2)のユーザ認証結果がOKの場合）、認証判断部123は、頂点(4)（“パスワード&ICカード”）の状態へ移行する。

【0059】上述のように、認証判断部123は、複数のユーザ認証部122(1)、122(2)、・・・、122(n)による複数のユーザ認証結果に基づいて、ユーザ認証状態を遷移させることで、最終的なユーザ認証判断結果を段階的に決定する。

【0060】＜サーバ120のサービスデータベース130の構成＞サービスデータベース130は、コンテンツ及びコンテンツに対する動作を含むサービスを保管するためのものであると共に、ユーザ認証判断結果、及びサービスに対応したアクセス制御リストを保管するためのものである。サーバ120は、サービスデータベース130内の保管情報（ユーザ認証判断結果情報及びアクセス制御リスト等）に基づいて、サービス提供部121により、サービス提供を制御する。

【0061】サービスデータベース130で管理するアクセス制御リストについては、例えば、パスワードを用いたユーザ認証、ICカードを用いたユーザ認証、及び指紋を用いたユーザ認証の3つのユーザ認証結果に基づいて、最終的なユーザ認証判断結果を決定する場合、当該アクセス制御リストは、3次元的な構成をなすリストとなる。

【0062】図4は、上記の場合において、コンテンツが画像コンテンツである場合のアクセス制御リストの一例を示したものである。上記図4において、縦軸の“頂点(0)～(7)”は、認証判断部123の最終的なユーザ認証判断結果を示す。

【0063】具体的には例えば、ここでは、パスワードを用いたユーザ認証、ICカードを用いたユーザ認証、及び指紋を用いたユーザ認証の3つのユーザ認証結果から最終的なユーザ認証結果を決定するため、上記図3に示したユーザ認証状態遷移が想定される。したがって、上記図4では、当該ユーザ認証状態遷移を縦軸としている。また、上記図4において、横軸は、画像コンテンツに対する多様化したサービスの示す。ここでは、「低解像度表示」、「高解像度表示」、「低解像度編集」、及び「高解像度編集」の4段階のサービスとしている。そして、縦軸（ユーザ認証状態）と、横軸（サービス）との交点の“○”（サービス許可）或いは“×”（サービス不許可）は、当該サービスを許可するか否か（画像コンテンツの表示或いは編集の動作）を示している。

【0064】尚、ここでは、画像コンテンツの表示及び編集のサービスを提供するものとし、アクセス制御リストを、上記図4に示したようなリストとしているが、これに限られることはない。例えば、画像コンテンツの印刷のサービスを提供するようにしてもよい。また、サービスの段階についても上記図4に示したものに限られる

ことはなく、例えば、「中解像度のコンテンツを印刷する」等のような、他の様々な形態のサービスを存在させるようにしてもよい。

【0065】また、上記図4に示したように、本実施の形態では、ユーザ認証判断結果、すなわち、上記図3に示したユーザ認証状態遷移における頂点(x)の位置によって、サービスの許可／不許可（アクセス制御）を決定することを特徴としているが、上記図4に示したようなアクセス制御リストに関しては特に制限しない。

【0066】例えば、図5に示すようなアクセス制御リストにより、アクセス制御を決定するようにしてもよい。この場合、全てのユーザ認証でユーザ認証結果がOKでない限り、サービスが許可されない。これにより、最も強固なユーザ認証を実現することができる。

【0067】また、例えば、図6に示すようなアクセス制御リストにより、アクセス制御を決定するようにしてもよい。この場合、何れか1つのユーザ認証でユーザ認証結果がOKである場合、画像コンテンツの表示に関するサービスが全て許可される。また、何れか2つのユーザ認証でユーザ認証結果がOKである場合、画像コンテンツの編集に関するサービスをも全て許可される。すなわち、この場合、全てのユーザ認証でのユーザ認証結果がOKでなくても、1つ或いは2つのユーザ認証でのユーザ認証結果がOKであれば、該当する段階（レベル）のサービスを受けることが可能となる。これにより、例えば、ユーザ認証に必要なICカードの紛失や盗難等の認証情報の保管に関する信頼性を向上させることができる。

【0068】また、例えば、図7に示すようなアクセス制御リストにより、アクセス制御を決定するようにしてもよい。この場合、ICカードの利用を前提とするシステム設計の要求に応じることができる。具体的には例えば、セキュリティを考慮したシステムにおいては、ICカードを利用したシステムが実用化されている。このことから、ICカードの利用を前提とするシステム設計が要求されることが考えられる。したがって、上記図7のアクセス制御リストを生成することで、上記の要求を実現できる。

【0069】上記図7のアクセス制御リストでは、ICカードを用いたユーザ認証結果がOKである場合、すなわち頂点(2)、頂点(4)、頂点(6)、及び頂点(7)（上記図3参照）の各ユーザ認証状態においては、サービスが全てを許可されるが、他の頂点のユーザ認証状態では、全てのサービスが許可されない。

【0070】また、上記図7のアクセス制御リストと共に、上記図6のアクセス制御リストを用いて、アクセス制御を決定するようにしてもよい。この場合、例えば、ユーザは、ICカードがない場合であっても、単一又は複数のICカード以外の、ユーザ認証を行うための手段（パスワードや指紋等）を用いて、ICカードによるユ

ユーザ認証の結果により許可されるサービスと同等のサービスを受けることができる。

【0071】＜ネットワークシステム100の動作＞図8は、ネットワークシステム100の動作を示したものである。例えば、ユーザ側の端末装置110(n)及びサーバ120が備えるコンピュータ機能200において、CPU201は、上記図8のフローチャートに従った処理プログラムを実行する。これにより、ネットワークシステム100は、次のように動作する。

【0072】ステップS301：ユーザは、自端末装置110(n)により、サーバ120に対してサービス要求(ユーザ認証要求)を発行する。

【0073】ステップS302：サーバ120において、複数のユーザ認証部122(1)、122(2)、・・・、122(n)の中の該当するユーザ認証部(以下、「ユーザ認証部122(x)」とする)は、ユーザ側の端末装置110(n)からの要求を受け付ける。例えば、ユーザがパスワード入力により当該要求を発行した場合には、パスワードによるユーザ認証を行うユーザ認証部122(1)が当該要求を受け付ける。認証判断部123は、ユーザ認証部122(x)で受け付けられた要求に基づいたユーザ認証結果に従って、上記図3に示したようなユーザ認証状態を遷移させる。

【0074】ステップS303：ユーザは、自端末装置110(n)により、他のユーザ認証方法によりサーバ120に対してサービス要求(ユーザ認証要求)する場合、当該サービス要求をサーバ120に対して発行する。この場合、再びステップS301からの処理が繰り返し実行される。一方、ユーザが、他のユーザ認証方法によりサーバ120に対してサービス要求(ユーザ認証要求)しない場合、次のステップS304からの処理に進む。

【0075】ステップS304：サーバ120において、認証判断部123は、ステップS301及びS302の結果(単一又は複数のユーザ認証結果に基づいた最終的なユーザ認証状態の遷移結果)を定める。

【0076】ステップS305：サービス提供部121は、認証判断部123で得られた最終的なユーザ認証判断結果、及び上記図4等に示したアクセス制御リストに基づいて、アクセス制御を決定し、該当するサービスを、ユーザ側の端末装置110(n)に対して許可、又は不許可する。

【0077】上述のように、本実施の形態では、複数のユーザ認証部122(1)、122(2)、・・・、122(n)によりユーザ認証を行い、それぞれのユーザ認証結果から、段階的なユーザ認証判断結果を最終的に決定し、そのユーザ認証判断結果に基づいて、段階的なサービスを提供するように構成した。すなわち、従来では、サービスに固定のユーザ認証方法のみが提供され、ユーザの認証結果に対して提供されるサービスが一意に

決まっていた構成に対して、本実施の形態では、段階的なユーザ認証判断結果を取得し、それに応じて適応的なサービスを提供することを実現した。これにより、ユーザのサービス享受の環境に適応的に対応してサービスを提供することができる。

【0078】[第2の実施の形態]本発明は、例えば、図9に示すようなネットワークシステム400(A)に適用される。本実施の形態のネットワークシステム400(A)は、特に、上記図9に示すように、上記図1に示したネットワークシステム100の構成に対して、2つのサーバ120(1)、120(2)を設けた構成が異なる。

【0079】尚、上記図9のネットワークシステム400(A)において、上記図1のネットワークシステム100と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【0080】すなわち、本実施の形態では、ユーザ認証を行うサーバ(認証サーバ)120(1)と、サービスを提供するサーバ(サービス提供サーバ)120(2)とを分けて設けるようにする。

【0081】サーバ120(1)は、複数のユーザ認証部122(1)、122(2)、・・・、122(n)及び認証判断部123を含み、サーバ120(2)は、サービス提供部121及びサービスデータベース130を含んでいる。そして、これらのサーバ120(1)、120(2)は、上記図1のサーバ120と同様に、ネットワーク140上に接続されている。

【0082】したがって、ユーザは、自端末装置110(n)により、サーバ120(1)に対して、サーバ120(2)からサービスを受けるためのユーザ認証要求を発行する。

【0083】サーバ120(1)は、ユーザ側の端末装置110(n)からの要求に基づいて、ユーザ認証を行い、その結果(最終的なユーザ認証判断結果)をサーバ120(2)へ送信する。サーバ120(2)は、サーバ120(1)からのユーザ認証判断結果に基づいて、ユーザ側の端末装置110(n)のアクセス制御を決定する。

【0084】[第3の実施の形態]本発明は、例えば、図10に示すようなネットワークシステム400(B)に適用される。本実施の形態のネットワークシステム400(B)は、特に、上記図10に示すように、上記図1に示したネットワークシステム100の構成に対して、2つのサーバ120(3)、120(4)を設けた構成が異なる。

【0085】尚、上記図10のネットワークシステム400(B)において、上記図1のネットワークシステム100と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【0086】すなわち、本実施の形態では、ユーザ認証

を行う2つのサーバ（認証サーバ）120（3）及び120（4）を分けて設けるようにする。

【0087】サーバ120（3）は、複数のユーザ認証部122（1）、122（2）、・・・、122（n）の中の単一又は複数のユーザ認証部（上記図10では、ユーザ認証部122（x）以外のユーザ認証部）、認証判断部123、サービス提供部121、及びサービスデータベース130を含んでいる。サーバ120（4）は、複数のユーザ認証部122（1）、122（2）、・・・、122（n）の中の単一又は複数のユーザ認証部（上記図10では、ユーザ認証部122（x））を含んでいる。そして、これらのサーバ120（3）、120（4）は、上記図1のサーバ120と同様に、ネットワーク140上に接続されている。

【0088】したがって、ユーザは、自端末装置110（n）により、サーバ120（3）或いはサーバ120（4）に対して、サーバ120（3）からサービスを受けるためのユーザ認証要求を発行する。

【0089】サーバ120（3）は、ユーザ側の端末装置110（n）からの要求に基づいて、外部のサーバ120（4）のユーザ認証部、或いは内部のユーザ認証部によりユーザ認証を行い、その結果（最終的なユーザ認証判断結果）に基づいて、ユーザ側の端末装置110（n）のアクセス制御を決定する。

【0090】尚、上記図9のネットワークシステム400（A）の構成、及び上記図10のネットワークシステム400（B）の構成を組み合わせる新たなネットワークシステムを構成するようにしてもよい。すなわち、ユーザ認証を行うサーバと、サービスを提供するサーバとを、それぞれ複数備えるネットワークシステムを構成してもよい。

【0091】〔第4の実施の形態〕本発明は、例えば、図11に示すようなネットワークシステム500に適用される。本実施の形態のネットワークシステム500は、上記図11に示すように、上記図1のネットワークシステム100に対して、サーバ120が接続しているネットワーク140（1）と、これに対して外部のネットワーク（外部ネットワーク）140（2）とを備えている。

【0092】このため、ネットワークシステム500のユーザ側の端末装置としては、ネットワーク（内部ネットワーク）140（1）を介してサーバ120へアクセスするユーザ側の端末装置110（1）、及び外部ネットワーク140（2）を介してサーバ120へアクセスするユーザ側の端末装置110（2）が存在する。

【0093】また、サーバ120は、上記図1に示した構成に加えて、さらに詳細は後述する位置検出部124を備える構成としている。

【0094】尚、上記図11のネットワークシステム500において、上記図1のネットワークシステム100

と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略する。

【0095】サーバ120において、位置検出部124は、サービス要求（ユーザ認証要求）を発行したユーザ側の端末装置の位置を検出（内部ネットワーク140（1）上に位置するか、外部ネットワーク140（2）上に位置するかを検出）する。

【0096】尚、上記の“ネットワーク上の位置”は、例えば、ユーザ側の端末装置のIPアドレス、或いはユーザ側の端末装置が存在するネットワーク名、或いはユーザ側の端末装置のネットワーク上での論理的な位置等を含む。また、位置検出部124での位置検出方法としては、例えば、ユーザ側の端末装置から別途送出された位置情報により位置を検出する方法、或いはIPケットから位置を検出する方法等のように、ユーザ側の端末装置から送られてきた情報により、自動的に当該端末装置の位置を検出する方法等が適用可能あるが、特に限定しない。

【0097】認証判断部123は、第1の実施の形態と同様に、複数のユーザ認証部122（1）、122（2）、・・・、122（n）によりユーザ認証を行い、それぞれのユーザ認証結果から、段階的なユーザ認証判断結果を最終的に決定するが、この決定の際に、位置検出部124での検出結果をも含めて、当該決定を行う。

【0098】例えば、位置検出部124において、ユーザ認証要求を発行したユーザ側の端末装置が、サーバ120と同じネットワーク140（1）上に存在する、と検出された場合、認証判断部123は、基準を低くして（アクセス制御リストでのサービス許可の基準を低くして）、上記のユーザ認証判断結果を決定する。また、位置検出部124において、ユーザ認証要求を発行したユーザ側の端末装置が、サーバ120と異なるネットワーク140（2）上に存在する、と検出された場合、認証判断部123は、基準を高くして（アクセス制御リストでのサービス許可の基準を高くして）、上記のユーザ認証判断結果を決定する。

【0099】具体的には例えば、まず、図12は、上記図11のネットワークシステム500を、社内システム500に適用した場合の構成を示したものである。この場合、サーバ120が「社内サーバ」として機能し、ネットワーク（内部ネットワーク）140（1）が社内ネットワークとして機能し、ネットワーク（外部ネットワーク）140（2）が社外ネットワークとして機能する。また、社内ネットワーク140（1）上のユーザ側の端末装置110（1）が、社内の社員が使用する端末装置に相当し、社外ネットワーク140（2）上のユーザ側の端末装置110（2）が、社外の者が使用する端末装置に相当する。

【0100】図13及び図14は、上記図12の社内シ

システム500において、パスワードを用いたユーザ認証、ICカードを用いたユーザ認証、及び指紋を用いたユーザ認証の3つのユーザ認証結果から最終的なユーザ認証結果を決定するものとし、且つコンテンツを画像コンテンツとした場合の、アクセス制御リストの一例を示したものである。

【0101】上記図13のアクセス制御リストは、社内ネットワーク140(1)上に接続されたユーザ側の端末装置110(1)からのユーザ認証要求に対するアクセス制御リストであり、このアクセス制御リストにおいては、ユーザ側の端末装置110(1)に対して、1つ以上のユーザ認証でのユーザ認証結果がOKであれば、該当するサービスが許可される。

【0102】上記図14のアクセス制御リストは、社外ネットワーク140(2)上に接続されたユーザ側の端末装置110(2)からのユーザ認証要求に対するアクセス制御リストであり、このアクセス制御リストにおいては、ユーザ側の端末装置110(2)に対して、3つの全てのユーザ認証でのユーザ認証結果がOKでないと、該当するサービスが許可されない。

【0103】したがって、認証判断部123は、位置検出部124の検出結果が、ユーザ認証要求を発行したユーザ側の端末装置がサーバ120と同じネットワーク140(1)上に存在するという結果である場合、上記図13のアクセス制御リストにより、サービス提供許可の基準を低くして、最終的なユーザ認証判断結果を決定する。また、認証判断部123は、位置検出部124の検出結果が、ユーザ認証要求を発行したユーザ側の端末装置がサーバ120と異なるネットワーク140(2)上に存在するという結果である場合、上記図14のアクセス制御リストにより、サービス提供許可の基準を高くして、最終的なユーザ認証判断結果を決定する。

【0104】上述のように、本実施の形態では、認証判断部123にて最終的なユーザ認証判断結果を決定する際に、複数のユーザ認証部122(1)、122

(2)、・・・、122(n)による複数のユーザ認証結果だけでなく、ユーザ認証の対象となっているユーザ側の端末装置の位置情報を加味して、当該決定を行うように構成したので、より柔軟にユーザ認証のレベルを決定することができる。

【0105】尚、本発明の目的は、第1～第4の実施の形態のホスト及び端末の機能を実現するソフトウェアのプログラムコードを記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ(又はCPUやMPU)が記憶媒体に格納されたプログラムコードを読みだして実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が第1～第4の実施の形態の機能を実現することとなり、そのプログラムコードを記憶した記憶媒体は本発明を構成することとな

る。プログラムコードを供給するための記憶媒体としては、ROM、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード等を用いることができる。また、コンピュータが読みだしたプログラムコードを実行することにより、第1～第4の実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOS等が実際の処理の一部又は全部を行い、その処理によって第1～第4の実施の形態の機能が実現される場合も含まれることは言うまでもない。さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部又は全部を行い、その処理によって第1～第4の実施の形態の機能が実現される場合も含まれることは言うまでもない。

【0106】

【発明の効果】以上説明したように本発明では、ユーザからの要求(パスワードやICカード等による任意のサービス提供要求等)に基づいて、当該ユーザの認証を行う際に、単一又は複数のユーザ認証方法(パスワードを用いたユーザ認証方法、ICカードを用いたユーザ認証方法、バイオメトリクスを用いたユーザ認証方法等)による単一又は複数のユーザ認証結果に基づいて、最終的なユーザ認証結果を段階的に決定するように構成した。具体的には例えば、従来のように1つのユーザ認証方法に依存した1種類の情報から得られる「可」又は「不可」の二値のユーザ認証結果ではなく、複数のユーザ認証方法による複数のユーザ認証結果の組み合わせに基いて、多値のユーザ認証結果を出力できるように構成した。これにより、段階的なユーザ認証結果に基づいて、サービスの質を段階的に変える等して、ユーザにサービスを提供することができる。

【0107】また、上記の最終的なユーザ認証結果を段階的に決定する際に、ユーザからの要求がなされた装置或いはシステム等の存在位置をも加味するように構成した場合、より柔軟にユーザ認証結果の段階を決定することができる。

【0108】したがって、本発明によれば、

(1) 多様なサービス提供形態に対応できる。

(2) 段階的であって多様なサービスを提供する際に、それぞれのサービスに対応可能である。

(3) ユーザ認証結果に応じて適応的に異なるサービスを提供できる。という効果を得ることができる。

【図面の簡単な説明】

【図1】第1の実施の形態において、本発明を適用したネットワークシステムの構成を示すブロック図である。

【図2】上記ネットワークシステム内のサーバ及びユーザ側の端末装置が有するコンピュータ機能の構成を示すブロック図である。

【図3】上記サーバにおいて、認証判断部が最終的なユーザ認証判断結果を決定する際の、ユーザ認証状態の遷移を説明するための図である。

【図4】上記サーバにおいて、サービス提供部が上記ユーザ認証判断結果に基づいて段階的なサービス許可／不許可を決定するためのアクセス制御リストを説明するための図である。

【図5】上記アクセス制御リストの他の例（例1）を説明するための図である。

【図6】上記アクセス制御リストの他の例（例2）を説明するための図である。

【図7】上記アクセス制御リストの他の例（例3）を説明するための図である。

【図8】上記ネットワークシステムの動作を説明するためのフローチャートである。

【図9】第2の実施の形態において、本発明を適用したネットワークシステムの構成を示すブロック図である。

【図10】第3の実施の形態において、本発明を適用したネットワークシステムの構成を示すブロック図である。

【図11】第4の実施の形態において、本発明を適用し

たネットワークシステムの構成を示すブロック図である。

【図12】上記ネットワークシステムを社内システムに適用した場合の構成を示すブロック図である。

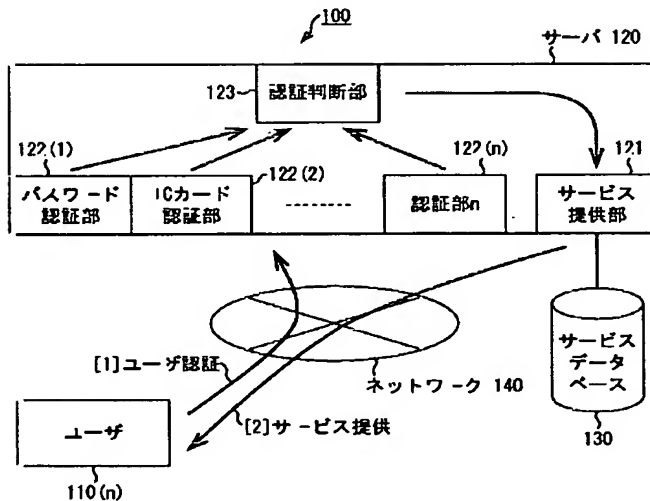
【図13】上記社内システムのサーバにおいて、サービス提供部がユーザ認証判断結果に基づいて段階的なサービス許可／不許可を決定するためのアクセス制御リスト（社内からのユーザ認証要求の場合のリスト）を説明するための図である。

【図14】上記社内システムのサーバにおいて、サービス提供部がユーザ認証判断結果に基づいて段階的なサービス許可／不許可を決定するためのアクセス制御リスト（社外からのユーザ認証要求の場合のリスト）を説明するための図である。

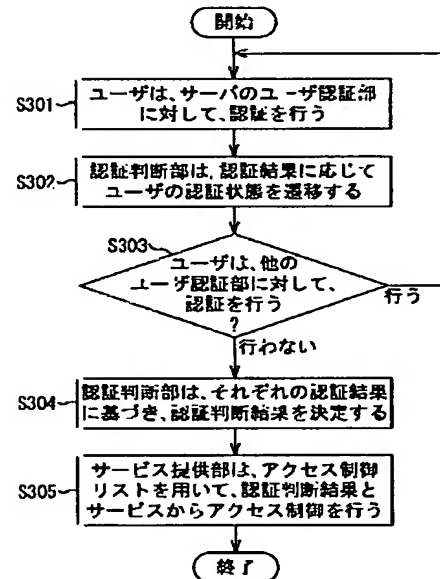
#### 【符号の説明】

- 100 ネットワークシステム
- 110 (n) ユーザ側の端末装置
- 120 サーバ
- 121 サービス提供部
- 122 (1), 122 (2), ..., 122 (n) ユーザ認証部
- 123 認証判断部
- 130 サービスデータベース
- 140 ネットワーク

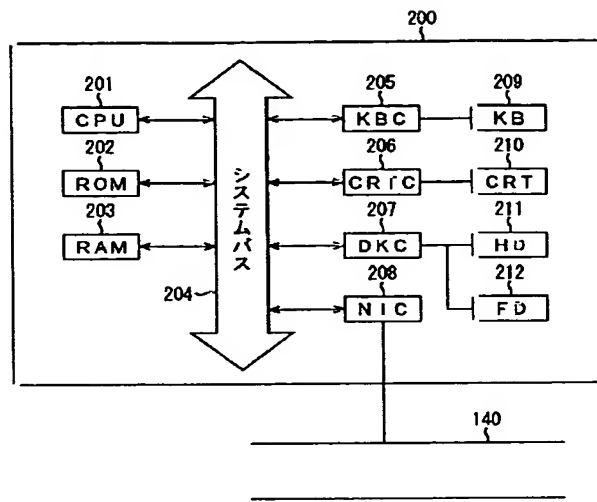
【図1】



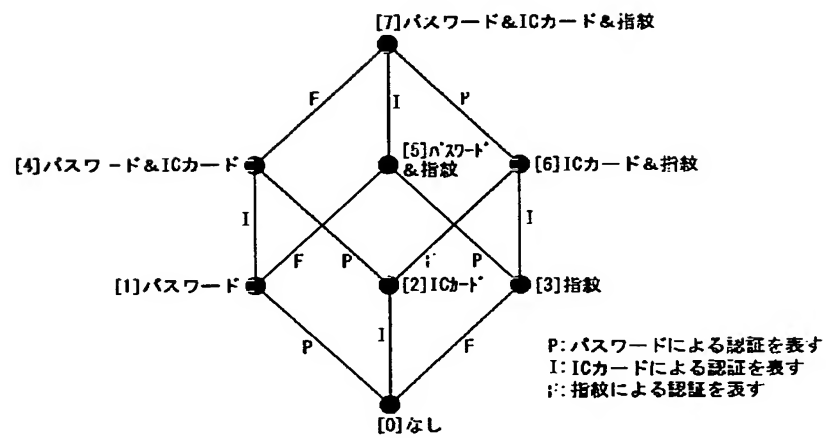
【図8】



【図2】



【図3】





【図4】

○：サービスを許可  
 ×：サービスを不許可

	低解像度 表示	高解像度 表示	低解像度 編集	高解像度 編集
頂点0	×	×	×	×
頂点1	○	×	×	×
頂点2	○	×	×	×
頂点3	○	×	×	×
頂点4	○	○	×	×
頂点5	○	○	○	×
頂点6	○	○	○	×
頂点7	○	○	○	○

【図5】

○：サービスを許可  
 ×：サービスを不許可

	低解像度 表示	高解像度 表示	低解像度 編集	高解像度 編集
頂点0	×	×	×	×
頂点1	×	×	×	×
頂点2	×	×	×	×
頂点3	×	×	×	×
頂点4	×	×	×	×
頂点5	×	×	×	×
頂点6	×	×	×	×
頂点7	○	○	○	○

【図6】

○：サービスを許可  
 ×：サービスを不許可

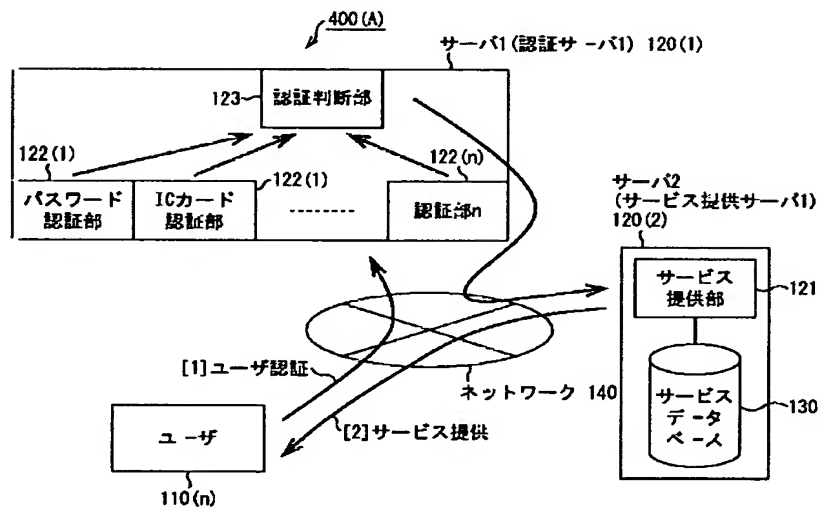
	低解像度 表示	高解像度 表示	低解像度 編集	高解像度 編集
頂点0	×	×	×	×
頂点1	○	○	×	×
頂点2	○	○	×	×
頂点3	○	○	×	×
頂点4	○	○	○	○
頂点5	○	○	○	○
頂点6	○	○	○	○
頂点7	○	○	○	○

【図7】

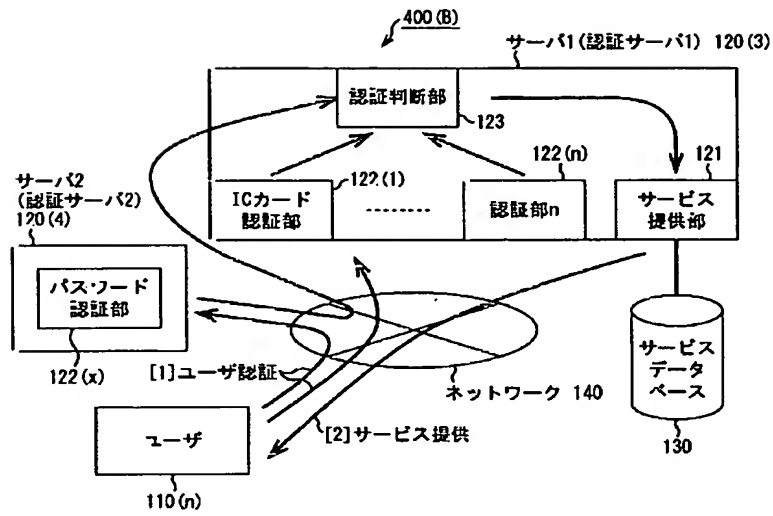
○：サービスを許可  
×：サービスを不許可

	低解像度 表示	高解像度 表示	低解像度 編集	高解像度 編集
頂点0	×	×	×	×
頂点1	×	×	×	×
頂点2	○	○	○	○
頂点3	×	×	×	×
頂点4	○	○	○	○
頂点5	×	×	×	×
頂点6	○	○	○	○
頂点7	○	○	○	○

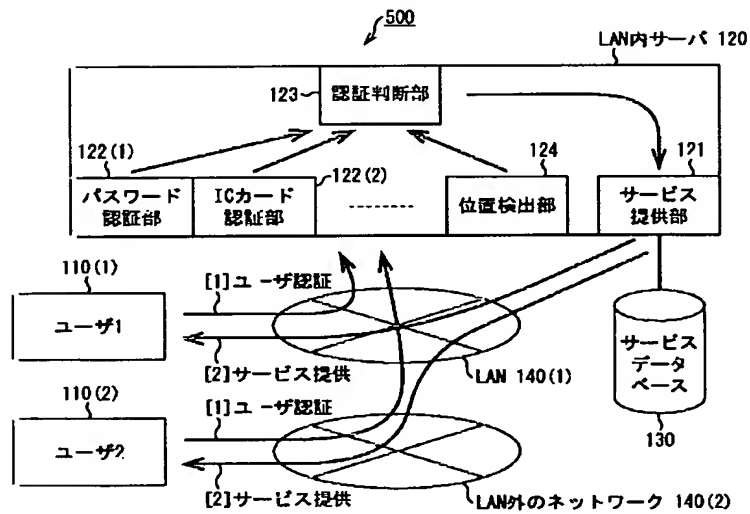
【図9】



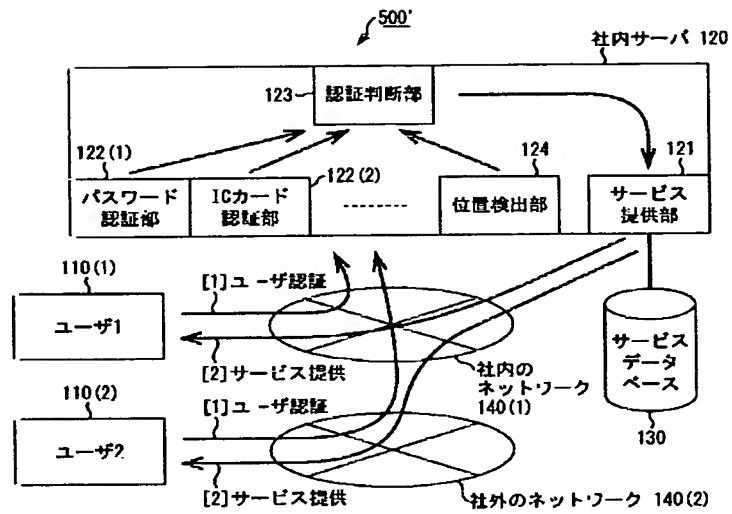
【図10】



【図11】



【 図 1 2 】



【 図 1 3 】

○：サービスを許可  
 ×：サービスを不許可

	低解像度 表示	高解像度 表示	低解像度 編集	高解像度 編集
社内ユーザ頂点0	×	×	×	×
社内ユーザ頂点1	○	○	○	○
社内ユーザ頂点2	○	○	○	○
社内ユーザ頂点3	○	○	○	○
社内ユーザ頂点4	○	○	○	○
社内ユーザ頂点5	○	○	○	○
社内ユーザ頂点6	○	○	○	○
社内ユーザ頂点7	○	○	○	○

【図 1 4】

○：サービスを許可  
 ×：サービスを不許可

	低解像度 表示	高解像度 表示	低解像度 編集	高解像度 編集
社外ユーザ頂点0	×	×	×	×
社外ユーザ頂点1	×	×	×	×
社外ユーザ頂点2	×	×	×	×
社外ユーザ頂点3	×	×	×	×
社外ユーザ頂点4	×	×	×	×
社外ユーザ頂点5	×	×	×	×
社外ユーザ頂点6	×	×	×	×
社外ユーザ頂点7	○	○	○	○

---

フロントページの続き

(72)発明者 若尾 聡  
 東京都大田区下丸子3丁目30番2号 キヤ  
 ノン株式会社内

Fターム(参考) 5B085 AE02 AE06 AE23  
 5J104 AA07 KA01 KA17 KA20 MA01  
 NA05 NA33 PA07

**THIS PAGE BLANK (USPTO)**